802.11g SIP DECT VoIP Router

VIP-462DG

User's manual

Copyright

Copyright (C) 2005 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

The is a class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks.

Revision

User’s Manual for PLANET 802.11g SIP VoIP Router:

Model: VIP-462DG

Rev: 1.0 (Sept. 2005)

Part No. EM-VIP462DGV1

Chapter 1 Introduction 6

Overview 6

Package Content 7

Physical Details 8

LED Display & Button 9

DCT-100 installation 11

Chapter 2 Preparations & Installation 12

Physical Installation Requirement 12

LAN/WAN Interface quick configurations 13

LAN IP address configuration via web configuration interface 13

WAN IP address configuration via web configuration interface 14

Chapter 3 Network Service Configurations 15

Configuring and monitoring your VIP-462DG from web browser 15

Overview on the web interface of VIP-462DG 15

Manipulation of VIP-462DG via web browser 15

Chapter 4 General Configurations 17

System Settings 17

Time Zone 17

Password Settings 17

Remote Management 18

WAN Settings 18

Dynamic IP 19

PPPoE 19

Static IP 20

DNS 20

LAN Settings 21

Wireless Setting 21

Channel and SSID 22

Security 22

Chapter 5 24

System Configurations 24

VoIP Settings 24

Port Setting 24

SIP Setting 25

VoIP adanced setting 25

Port advanced Setting and register DECT handset 26

Qos Settings 26

Traffic mapping 27

Traffic Statistics 28
NAT Settings 28
Address Mapping 29
Virtual Server 29
Special Application 31
Firewall Setting 32
Access Control 32
MAC Filter 34
URL Blocking 34
Schedule Rule 35
Intrusion Detection 36
DMZ 37
UPnP 38
DDNS 38
Tools 39
Configuration Tools 39
Firmware Upgrade 39
Reset 40
Status 40
Internet Connection 40
Device Status 41
Security Log 41
DHCP Clinet Log 41
VoIP Status 42
Appendix A 43
VIP-462DG Specifications 43

Chapter 1 Introduction

Overview

Combining cutting edge Internet telephony and router manufacturing experience, PLANET proudly introduces the newest member of the PLANET VoIP gateway family: the VIP-462DG.

To bring the most satisfaction to customers, the VIP-462DG, not only provides quality voice communications, wired/wireless Internet sharing capabilities, but also offers DECT interface for daily wireless telephony communications. With advanced router/firewall, and VoIP DSP processor technology, the VIP-462DG is able to make calls via SIP proxy voice communications, plus the IP sharing, QoS, and the SPI firewall mechanism, VIP-462DG is the ideal choice for Voice over IP communications and providing integrated Internet sharing for the daily tasks. To bring the users most flexibility, the add-on RJ-11 interface for PSTN connection, users not only can make the daily PSTN communication, but also enjoy the convenience brought by VoIP communications.

With built-in DECT & GAP Compatible base, up to 5 DECT handset can be registered on the VIP-462DG. The pan European users can be benefit from the DECT interface, voice communications can be established from anywhere in the living space. The PLANET VIP-462DG comes with an intuitive, user-friendly, yet powerful web management interface, no expertise required for the VoIP communications.

Firewall/Security Feature

- Built in NAT firewall, DoS (Denial of Service) protection
- QoS mechanism to ensure the voice quality
- SPI (Stateful Packet Inspection) firewall
- Policy-based LAN/WAN access control
- Virtual server, DMZ,
- Remote administrator authentication
- Scheduled access control

VoIP Functions

- SIP 2.0 (RFC3261) compliant
- SIP proxy calls
- Voice codec support: G.711, G.723.1A, G.729A
- Voice processing: Voice Active Detection, DTMF detection/ generation, G.168 echo cancellation (16mSec.), Comfort noise generation, Call progress detection, Gain Control
- PSTN lifeline for emergency calls

DECT Features

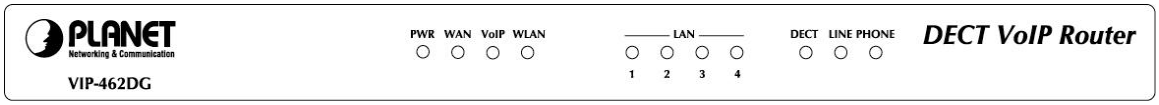
- DECT & GAP Compatible
- Base can register up to 8 Handsets
- Intercom call during external call, Call transfer between • handsets , three-way telephone meeting
- CID 50 locations
- Redial memory: 3 locations, 20 digits
- Adjustable ringer volume & melody
- 100 hours standby time, 8 hours talk time
- Hands-Free, Mute function
- Call duration time meter
- Transmitted distance: up to 50m indoor / up to 300m outdoor

Package Content

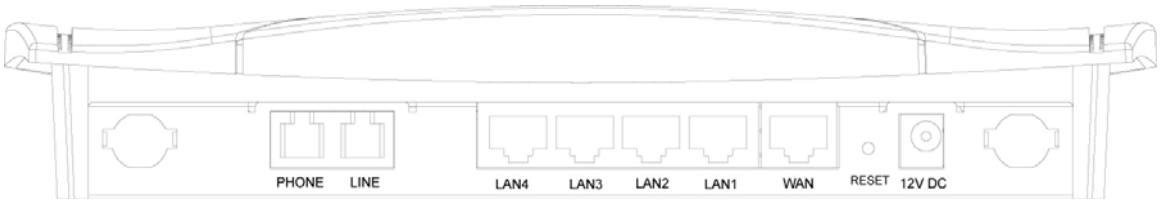
The contents of your product should contain the following items:
DECT VoIP router
DECT handset
DECT handset charger
Power handset power adapter
Quick Installation Guide
User's Manual CD
RJ-11 cable x 1
RJ-45 cable x 1

Physical Details

The following figure illustrates the front/rear panel of VIP-462DG.



Front Panel of VIP-462DG

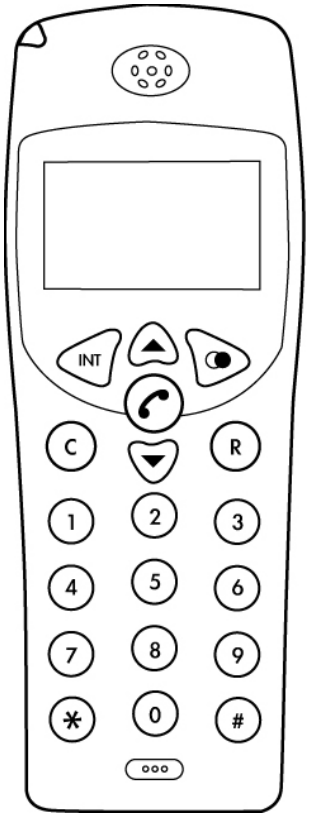


Rear Panel of VIP-462DG

LED Display & Button

LED Indicators	Descriptions
PWR	**Light (Green):** power on, normal operaion **Blink:** firmware loading **Off:** power off or failure
WAN	**Light (Green):** connection is active **Blink (Green):** data transmitting or receiving **Off:** connection is not established
VoIP	**Light (Orange):** SIP proxy registration is successful **Blink (Orange):** SIP proxy registration is unsuccessful **Off:** SIP proxy registration is disable
WLAN	**Light (Green):** connection is active
LAN 1 ~ LAN 4	**Light:** connection is active **Blink:** data transmitting or receiving **Off:** connection is not established
Phone	**Light (Green):** the phone is use (offhook) **Blink:** ring for incoming call **Off:** the phone is idle (onhook)
Line	**Light (Green):** the line is use (offhook) **Blink:** ring for incoming call **Off:** the line is idle (onhook)

Back Panels	Descriptions
DC12V	Power Adapter connecter
RESET (Reboot)	Press for one second to reset the device or press for 5 seconds to reset to the factory default.
WAN	10/100Mbps RJ-45 connector connect to ADSL or cable modem
LAN 1 ~ LAN 4	10/100Mbps RJ-45 connector connect to PC or local switch/hub.
LINE	Connect to the RJ-11 PSTN line
Phone	Connect to the RJ-11 phone line



Overview of DECT handset DCT-100

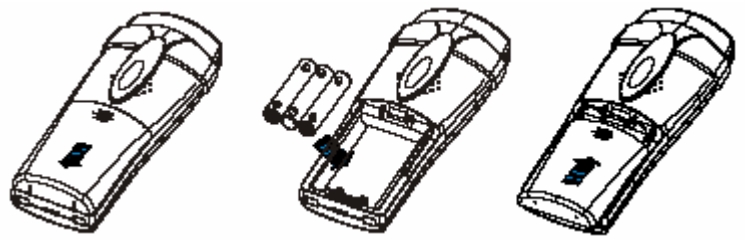
Keypad and button definition on DCT-100

	Descriptions
INT	Intercom conversation mode
	Adjust the volume level during the conversation and menu selection on the LCD display
	Last Number Redial
	Hang on / up telephone or pressing until to open /close speaker
C	Cancel and Clear
R	Power on / off
Number 0 –9 and #	The function is as the same as the general phone set
****	Press ** to switch to PSTN

DCT-100 installation

The three rechargeable Ni-MH batteries (AAA size) come with your phone. Install the batteries before using your phone.

1. Slide the battery cover in the direction of the arrow and pull it out.
2. Remove old batteries, if any, and insert new batteries as indicated, matching correct polarity (+, -).
3. Replace the battery cover, slide the cover up until it snaps shut.



Note

- This phone won't work by itself. It should be registered to the main base unit inside the VIP-320.
- Before initial using, it should be charged for 24 hours.

Note

- Reversing the orientation may damage the handset.
- The battery needs to be replaced if it does not recover its full storage capacity after recharging.
- When replacing batteries, always use good quality Ni-MH re-chargeable AAA size batteries.
- Never use other batteries or conventional alkaline batteries.

Chapter 2

Preparations & Installation

Physical Installation Requirement

This chapter illustrates basic installation of VIP-462DG

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.

For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage)

Administration Interface

PLANET VIP-462DG provides GUI (Web based, Graphical User Interface) for machine management and administration.

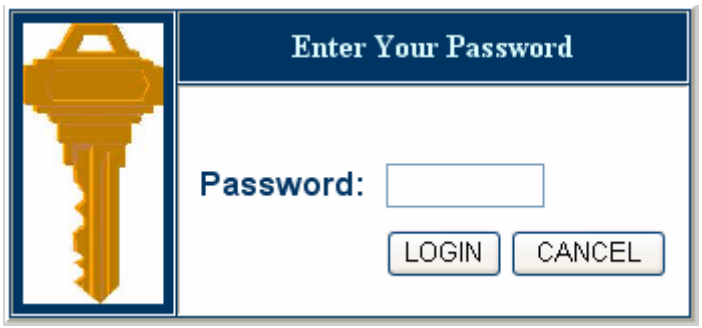
Web configuration access

To start VIP-462DG web configuration, you must have one of these web browsers installed on computer for management

- Netscape Communicator 4.03 or higher
- Microsoft Internet Explorer 5.5 or higher with Java support

Default LAN interface IP address of VIP-462DG is **192.168.0.1**. You may now open your web browser, and insert **192.168.0.1** in the address bar of your web browser to logon VIP-462DG web configuration page.

VIP-462DG will prompt for logon password, please enter: **123** to continue machine administration.



Note

Please locate your PC in the same network segment (192.168.0.x) of VIP-462DG. If you're not familiar with TCP/IP, please refer to related chapter on user's manual CD or consult your network administrator for proper network configurations.

LAN/WAN Interface quick configurations

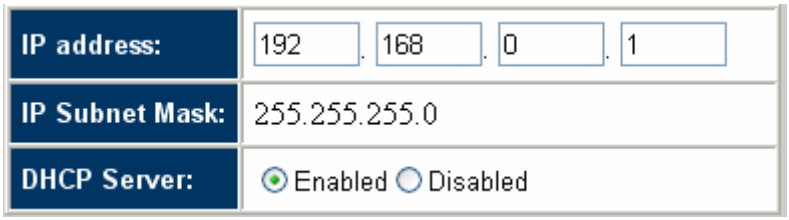
Nature of PLANET VIP-462DG is an IP Sharing (NAT) device, it comes with two default IP addresses, and default LAN side IP address is "**192.168.0.1**", default WAN side IP address is "**172.16.0.1**". You may use any PC to connect to the LAN port of VIP-462DG to start machine administration.

Hint

In general cases, the LAN IP address is the default gateway of LAN side workstations for Internet access, and the WAN IP of VIP-462DG is the IP address for remote calling party to connect with.

LAN IP address configuration via web configuration interface

Execute your web browser, and insert the IP address (default: **192.168.0.1**) of VIP in the adddress bar. After logging on machine with password (default: **123**), browse to "**LAN**" configuration menu:



Parameter Description

IP address LAN IP address of VIP-462DG

Default: 192.168.0.1

Subnet Mask LAN mask of VIP-462DG

Default: 255.255.255.0

After confirming the modification you've done, Please click on the **Apply** button to macke the changes effective.

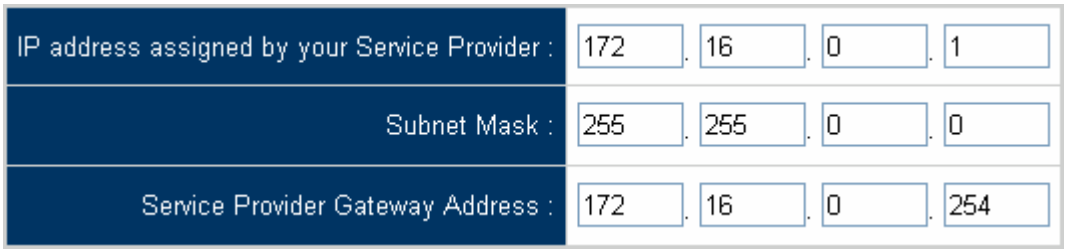
WAN IP address configuration via web configuration interface

Execute your web browser, and type **http://172.16.0.1** in the adddress bar.

ⓘ Hint

If you're using WAN port login the VIP-462DG, please be sure to check if the **"Rermote Management"** is enabled in machine.

After logging on machine with password (default: **123**), browse to "**WAN**" →"**Static IP**" configuration menu, you will see the configuration screen below:


IP address assigned by your Service Provider : 172 . 16 . 0 . 1
Subnet Mask : 255 . 255 . 0 . 0
Service Provider Gateway Address : 172 . 16 . 0 . 254

After confirming the modification you've done, Please click on the **Apply** button to macke the changes effective.

Connection Type	Data required.
Dynamic IP	Obtains an IP address automatically from your service provider.
PPPoE	PPP over Ethernet is a common connection method used for xDSL.
Static IP Address	The service provider provides a static IP address to access Internet services.

ⓘ Hint

Please consult your ISP personnel to obtain proper PPPoE/IP address related information, and input carefully.
If Internet connection cannot be established, please check the physical connection or contact the ISP service staff for support information.

Chapter 3

Network Service Configurations

Configuring and monitoring your VIP-462DG from web browser

The VIP-462DG integrates a web-based graphical user interface that can cover most configurations and machine status monitoring. Via standard, web browser, you can configure and check machine status from anywhere around the world.

Overview on the web interface of VIP-462DG

With web graphical user interface, you may have:

- More comprehensive setting feels than traditional command line interface.
- Provides user input data fields, check boxes, and for changing machine configuration settings
- Displays machine running configuration

To start VIP-462DG web configuration, you must have one of these web browsers installed on computer for management

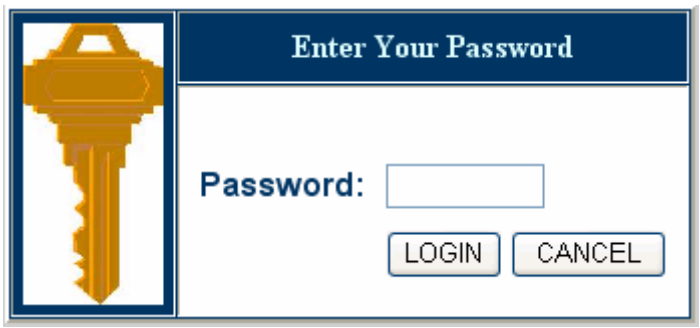
- Netscape Communicator 4.03 or higher
- Microsoft Internet Explorer 5.5 or higher with Java support

Manipulation of VIP-462DG via web browser

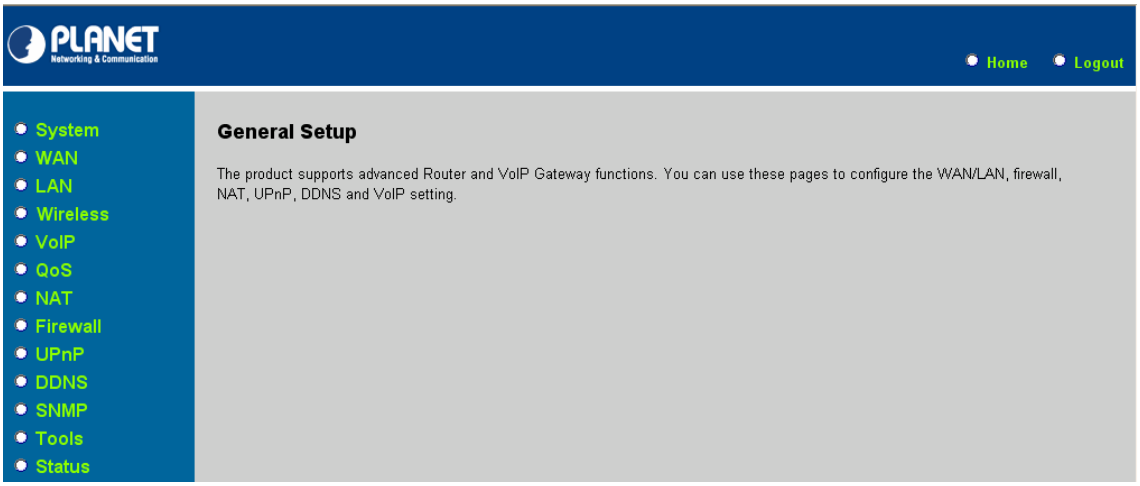
Log on VIP-462DG via web browser

After TCP/IP configurations on your PC, you may now open your web browser, and input ***http://192.168.0.1*** to logon VIP-462DG web configuration page.

VIP-462DG will prompt for logon password: ***123***



VIP-462DG log in page



VIP-462DG main page

Chapter 4

General Configurations

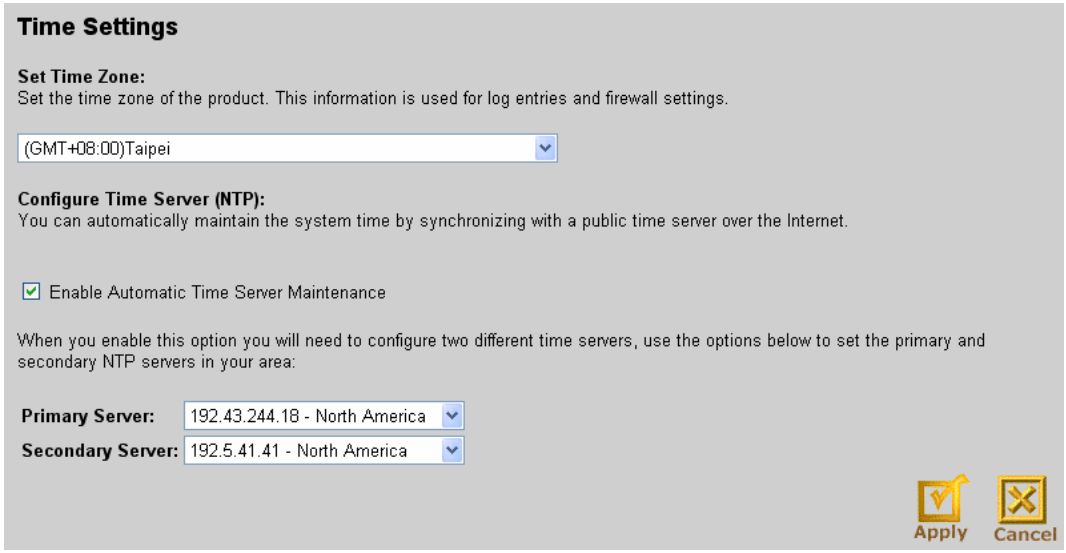
System Settings

This page includes all the basic configuration tools for the product, such as options to control management access.

Time Zone

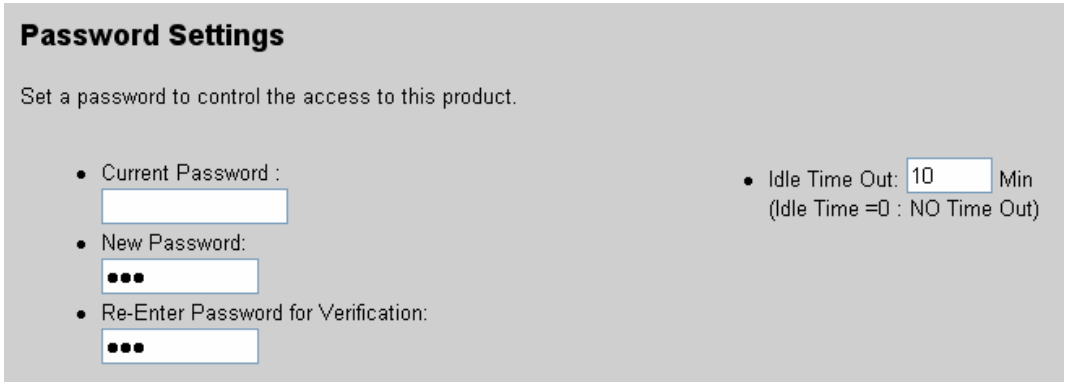
Set the proper time zone and the configure time server for the VIP-462DG.

When you enable “Automatic Time Server Maintenance” option you will need to configure time servers, use the options below to set the primary and secondary NTP servers in your area


Time Settings
Set Time Zone:
Set the time zone of the product. This information is used for log entries and firewall settings.
(GMT+08:00)Taipei
Configure Time Server (NTP):
You can automatically maintain the system time by synchronizing with a public time server over the Internet.
Enable Automatic Time Server Maintenance
When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:
Primary Server: 192.43.244.18 - North America
Secondary Server: 192.5.41.41 - North America
Apply
Cancel

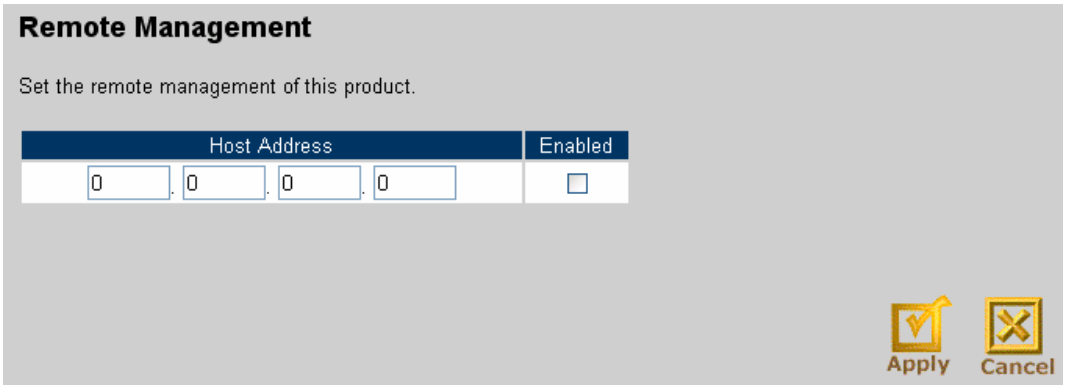
Password Settings

Set the password of the user. The Idle Time Out value is used for VIP-462DG to log out automatically when no access to the web after this timeout value.


Password Settings
Set a password to control the access to this product.
Current Password :
New Password:
Re-Enter Password for Verification:
Idle Time Out: 10 Min
(Idle Time =0 : NO Time Out)

Remote Management

The "Remote Management" feature can restrict remote user login from the WAN port. The IP setting of "0.0.0.0" allows user from any IP address to remote logged in to the device. When the 'Enabled" is not checked, remote login is disabled.



ⓘ Hint

The remote user can login using WAN IP. The default port number is **8080.**

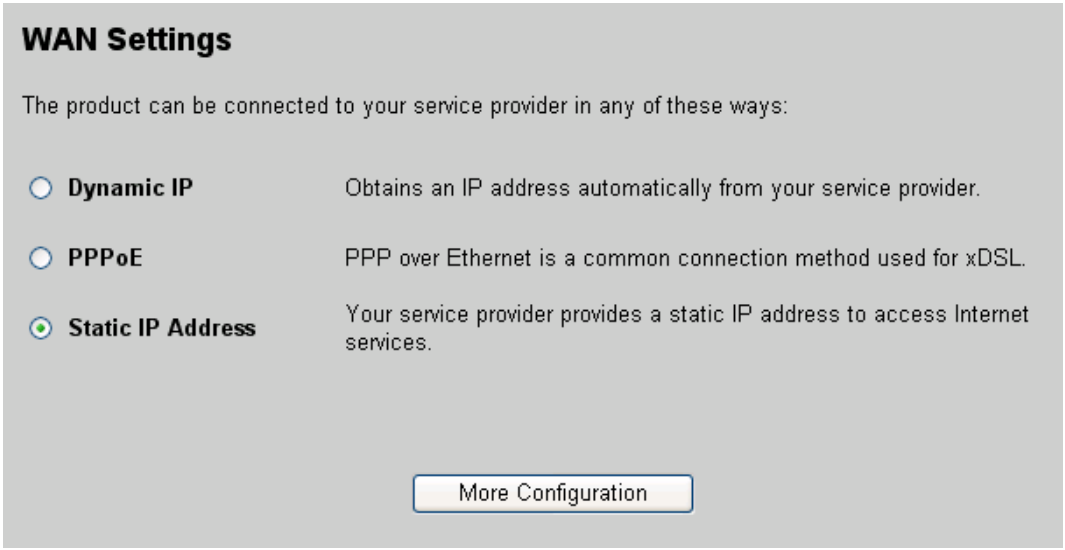
WAN Settings

The VIP-462DG supports 3 types of WAN connection:

Dynamic IP (DHCP Client)

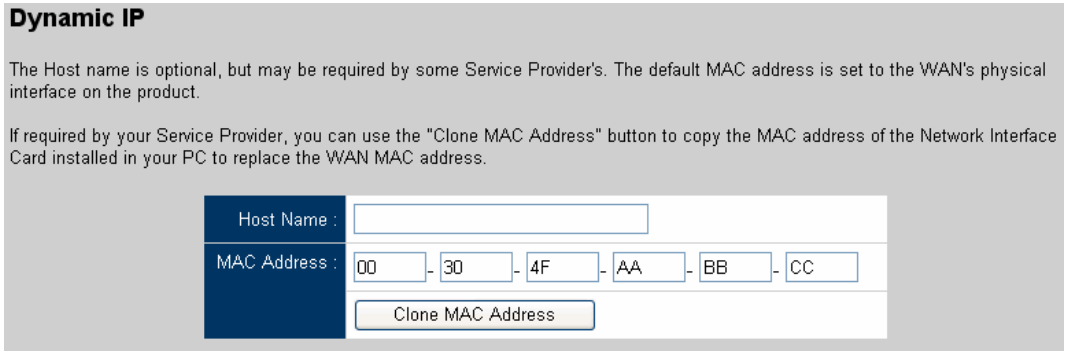
PPPoE

Static IP (factory deault value)


WAN Settings
The product can be connected to your service provider in any of these ways:
Dynamic IP
Obtains an IP address automatically from your service provider.
PPPoE
PPP over Ethernet is a common connection method used for xDSL.
Static IP Address
Your service provider provides a static IP address to access Internet services.
More Configuration

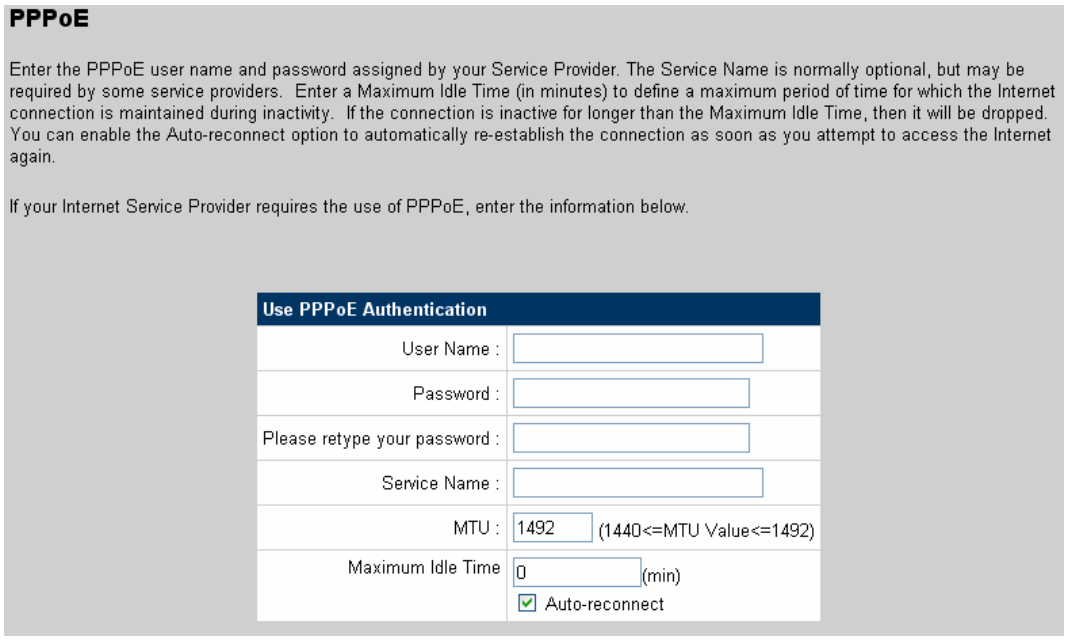
Dynamic IP

Under this mode, VIP-462DG enables DHCP client to get IP address automatically from your service provider. The Host Name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the VIP-462DG. If required by service provider, you use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC and replace the WAN MAC address with this MAC address. If necessary, you can use the "Restore" buttons to restore the WAN IP address.


Dynamic IP
The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the product.
If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.
Host Name :
MAC Address :
00 - 30 - 4F - AA - BB - CC
Clone MAC Address

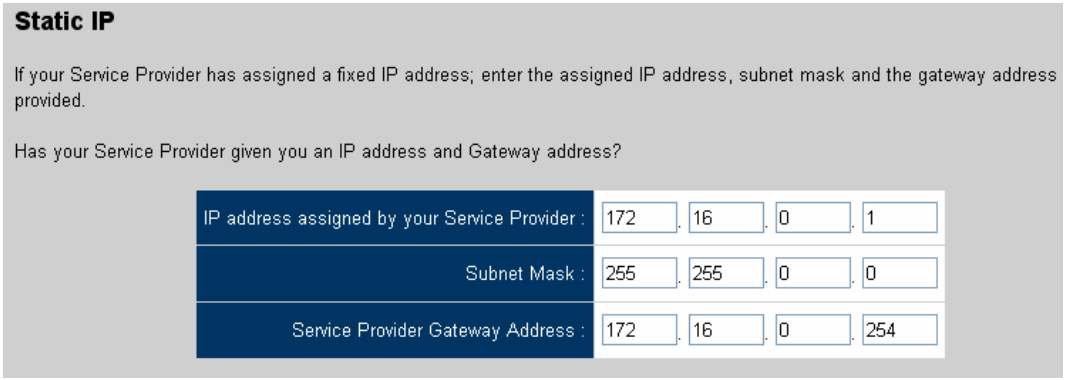
PPPoE

Under this mode, VIP-462DG is acting as a PPPoE client. Enter the PPPoE user name and password assigned by your service provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in seconds) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again


PPPoE
Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.
If your Internet Service Provider requires the use of PPPoE, enter the information below.
Use PPPoE Authentication
User Name :
Password :
Please retype your password :
Service Name :
MTU : 1492 (1440<=MTU Value<=1492)
Maximum Idle Time 0 (min)
Auto-reconnect

Static IP

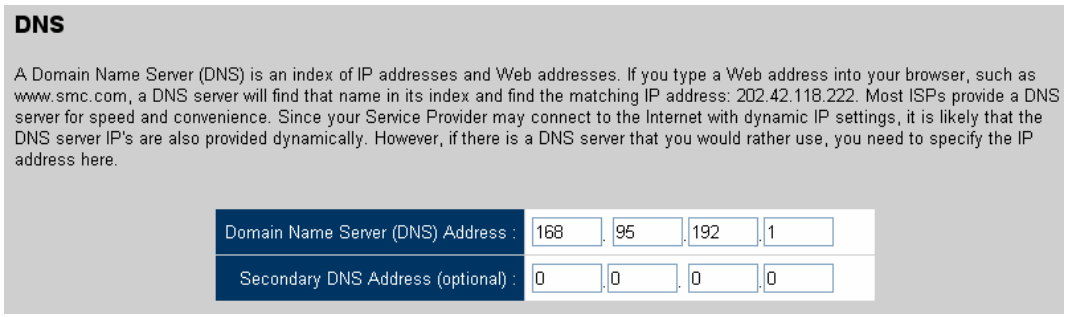
If your service provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided.


Static IP
If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.
Has your Service Provider given you an IP address and Gateway address?
IP address assigned by your Service Provider : 172 . 16 . 0 . 1
Subnet Mask : 255 . 255 . 0 . 0
Service Provider Gateway Address : 172 . 16 . 0 . 254

DNS

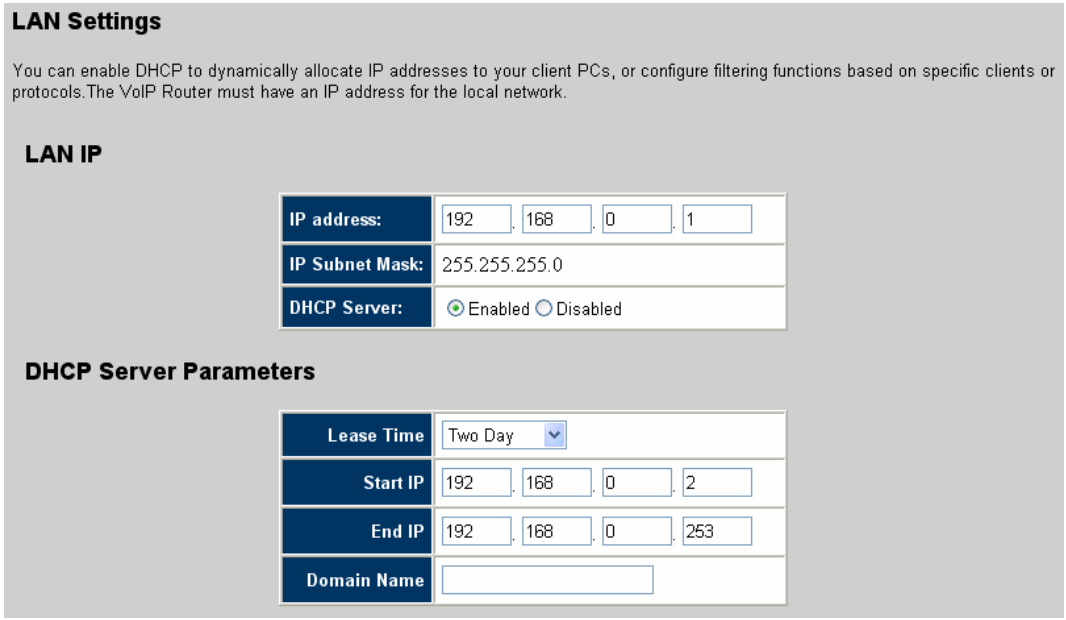
Most service providers provide a DNS server for speed and convenience. If there is a DNS server that you would rather use, you need to specify the IP address here. If you are static IP user, you must specify DNS server IP. When primary DNS does not work, system will use secondary DNS.

If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided.


DNS
A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 202.42.118.222. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.
Domain Name Server (DNS) Address : 168 . 95 . 192 . 1
Secondary DNS Address (optional) : 0 . 0 . 0 . 0

LAN Settings

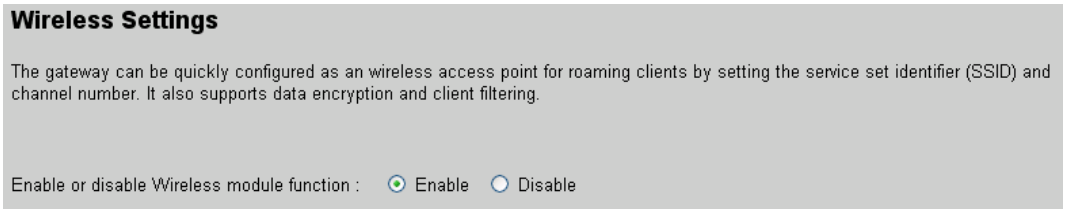
The VIP-462DG needs to have an IP address of the local network. You can enable DHCP to dynamically allocate IP addresses to your client PCs. When DHCP server is enabled, you need to enter the IP address range for the local hosts.


LAN Settings
You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols.The VoIP Router must have an IP address for the local network.
LAN IP
IP address: 192 . 168 . 0 . 1
IP Subnet Mask: 255.255.255.0
DHCP Server: Enabled Disabled
DHCP Server Parameters
Lease Time: Two Day
Start IP: 192 . 168 . 0 . 2
End IP: 192 . 168 . 0 . 253
Domain Name

The domain name field is empty in most case. In some special ISP need input domain name field.

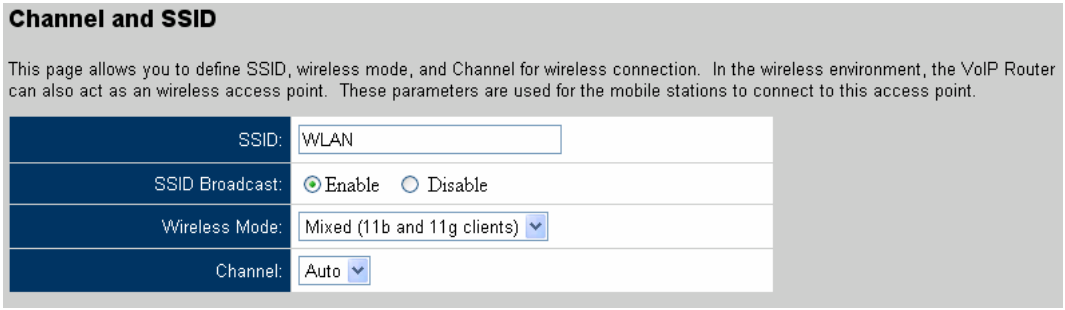
Wireless Setting

VIP-462DG can be quickly configured as a wireless access point for roaming clients by setting the service set identifier (SSID) and channel number. It also supports data encryption and client filtering.


Wireless Settings
The gateway can be quickly configured as an wireless access point for roaming clients by setting the service set identifier (SSID) and channel number. It also supports data encryption and client filtering.
Enable or disable Wireless module function : Enable Disable

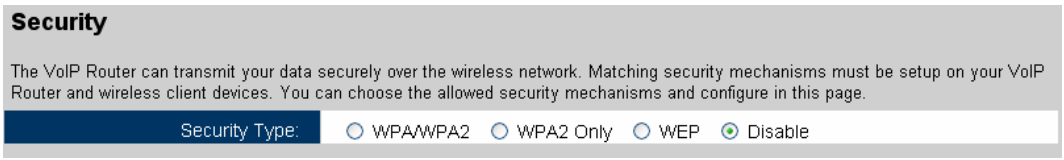
Channel and SSID

This page allows you to define SSID, Transmission Rate, Basic Rate and Channel ID for wireless connection. In the wireless environment, VIP-462DG can also act as a wireless access point. These parameters are used for the mobile stations to connect to this access point.


Channel and SSID
This page allows you to define SSID, wireless mode, and Channel for wireless connection. In the wireless environment, the VoIP Router can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.
SSID:
WLAN
SSID Broadcast:
Enable
Disable
Wireless Mode:
Mixed (11b and 11g clients)
Channel:
Auto

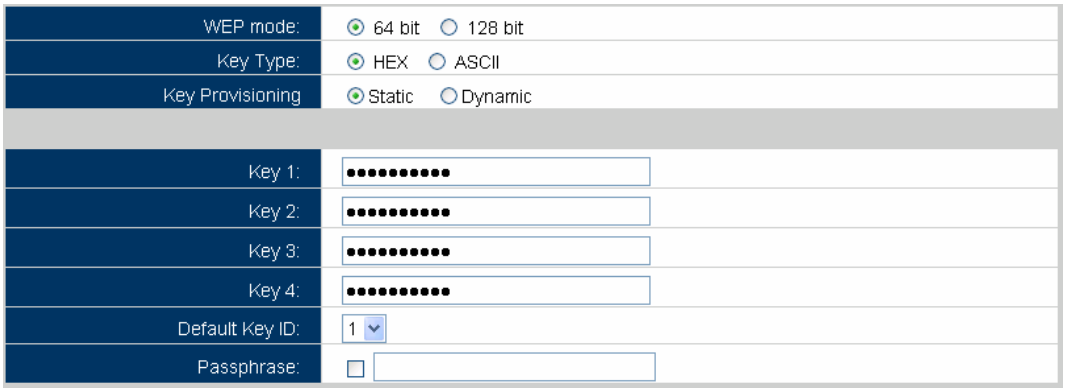
Security

VIP-462DG can transmit your data security over the wireless network. Matching security mechanisms must be setup on your VIP-462DG and wireless client devices. You can choose the allowed mechanisms in this page and configure them in the sub-pages.


Security
The VoIP Router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your VoIP Router and wireless client devices. You can choose the allowed security mechanisms and configure in this page.
Security Type:
WPA/WPA2
WPA2 Only
WEP
Disable

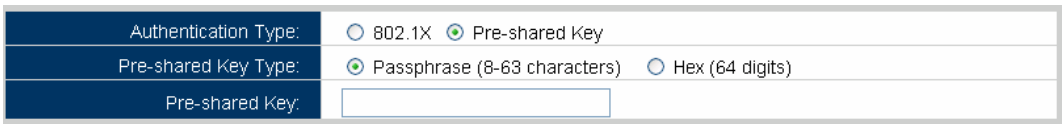
WEP

WEP is the basic mechanism to transmit you data security over the wireless network. Matching encryption keys must be setup on your VIP-462DG and wireless client device to use WEP



WPA

WPA is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your VIP-462DG and wireless client devices to use WPA.



Chapter 5

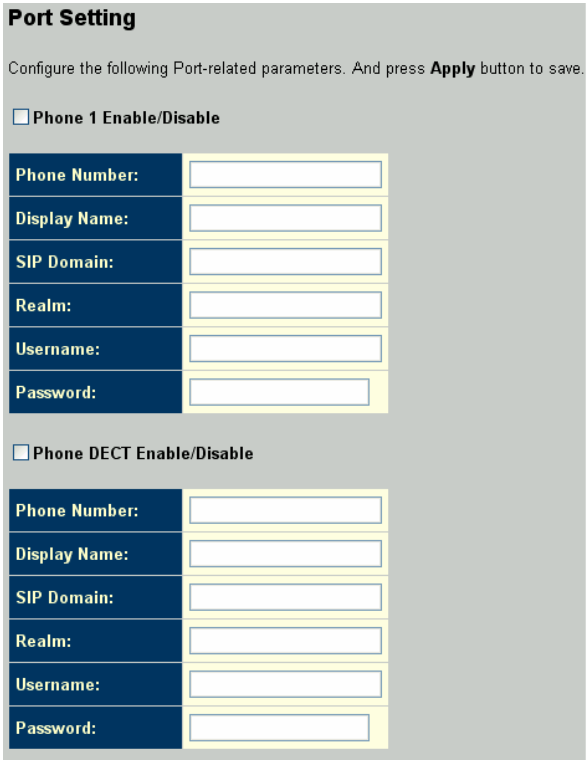
System Configurations

VoIP Settings

The section includes the entire VoIP configuration for VIP-462DG.

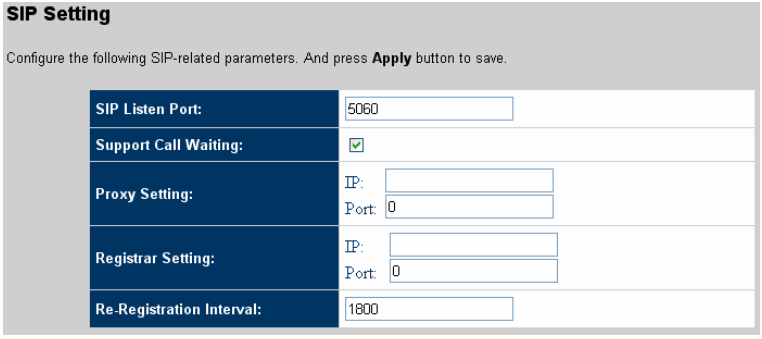
Port Setting

This page sets up the phone number and username/password for SIP server registration. The phone number and username/password must be predefined in SIP Proxy. You can register two VoIP number to VIP-462DG, register one number for analog telephone set and the other number for DECT handset.



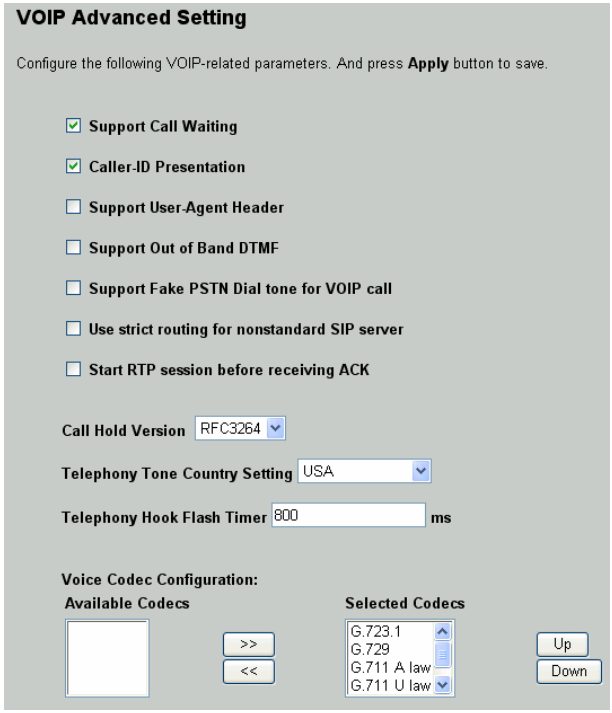
SIP Setting

This page defines the SIP parameters, in the SIP Parameters setting, we need to set SIP domain and SIP Proxy IP address. The default register expire time is 1800 second. So the system must reregister to SIP proxy again within register expire time.



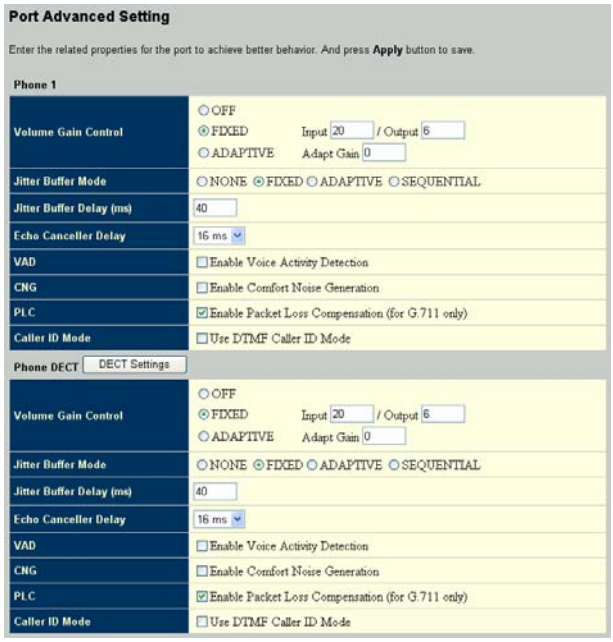
VoIP adanced setting

This page allows you to configure advanced VoIP features including voice Codec configuration.



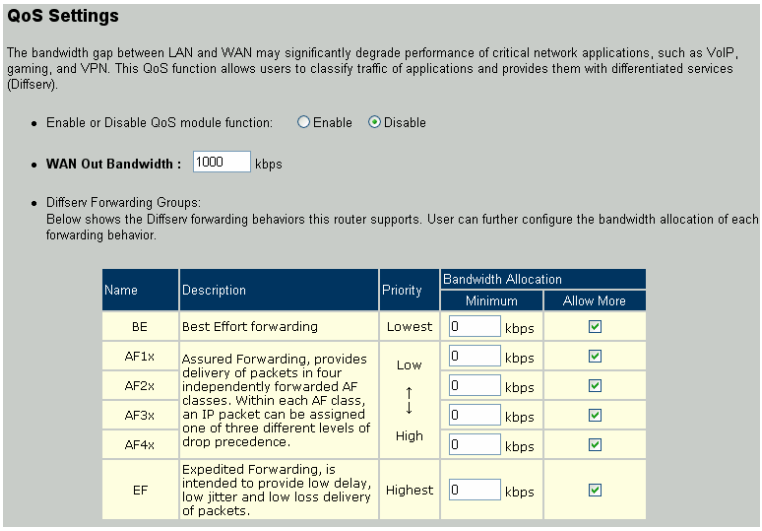
Port advanced Setting and register DECT handset

This page allows you adjust the parameter of voice channel to achieve better sound quality. In this page also provide DECT setting for you to paging and register new DECT handset.



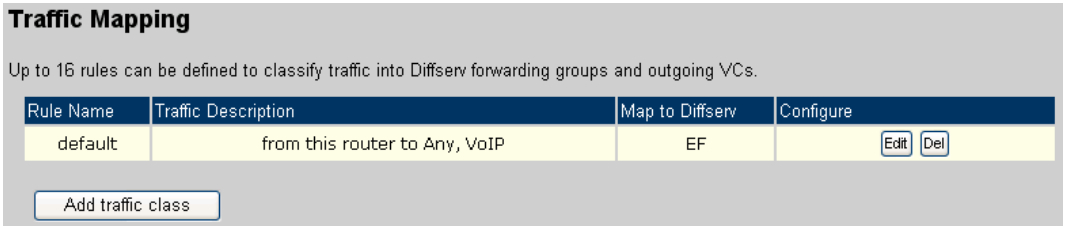
Qos Settings

The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming and VPN. This QoS function allows users to classify traffic of application and provide them with differentiated services (Difffserv).


QoS Settings
The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. This QoS function allows users to classify traffic of applications and provides them with differentiated services (Diffserv).
Enable or Disable QoS module function: Enable Disable
WAN Out Bandwidth : 1000 kbps
Diffserv Forwarding Groups:
Below shows the Diffserv forwarding behaviors this router supports. User can further configure the bandwidth allocation of each forwarding behavior.
Name
Description
Priority
Bandwidth Allocation
Minimum
Allow More
BE
Best Effort forwarding
Lowest
0 kbps
AF1x
Assured Forwarding, provides delivery of packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence.
Low
0 kbps
AF2x
0 kbps
AF3x
0 kbps
AF4x
High
0 kbps
EF
Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.
Highest
0 kbps

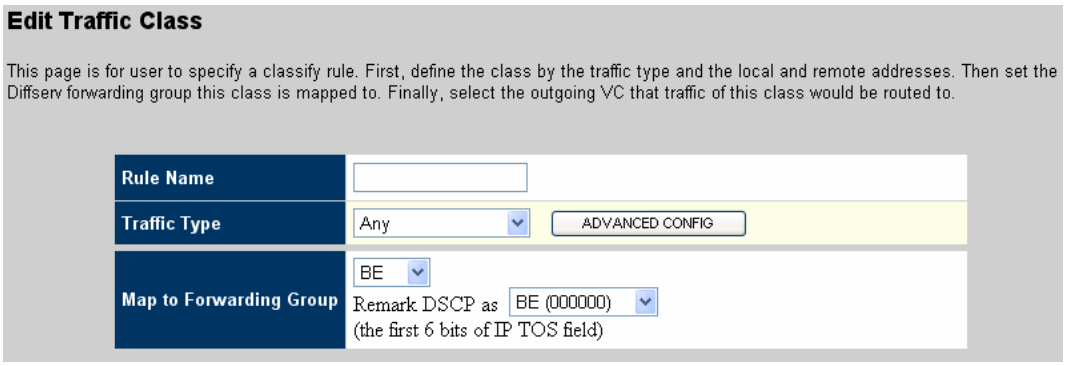
Traffic mapping

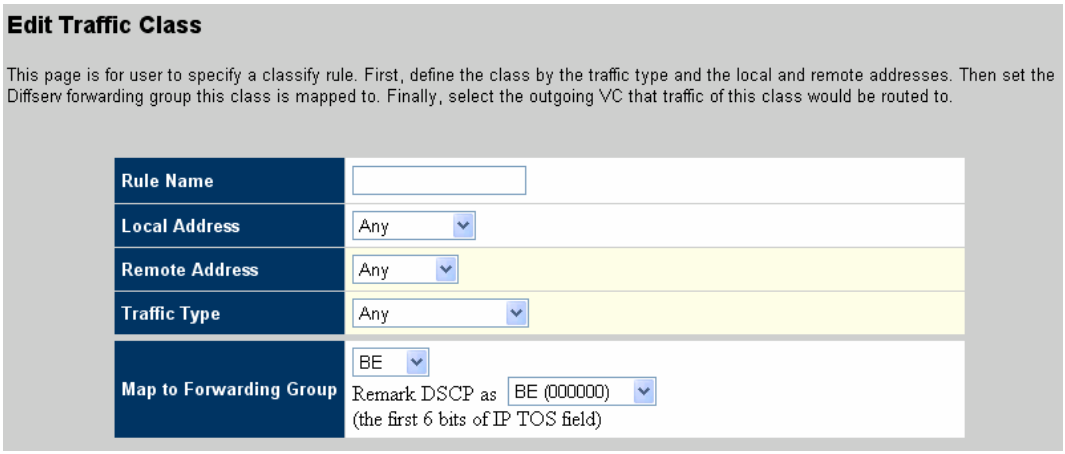
Up to 16 rules can be defined to classify traffic into Diffserv forwarding groups and outgoing VCs.



Edit Traffic class

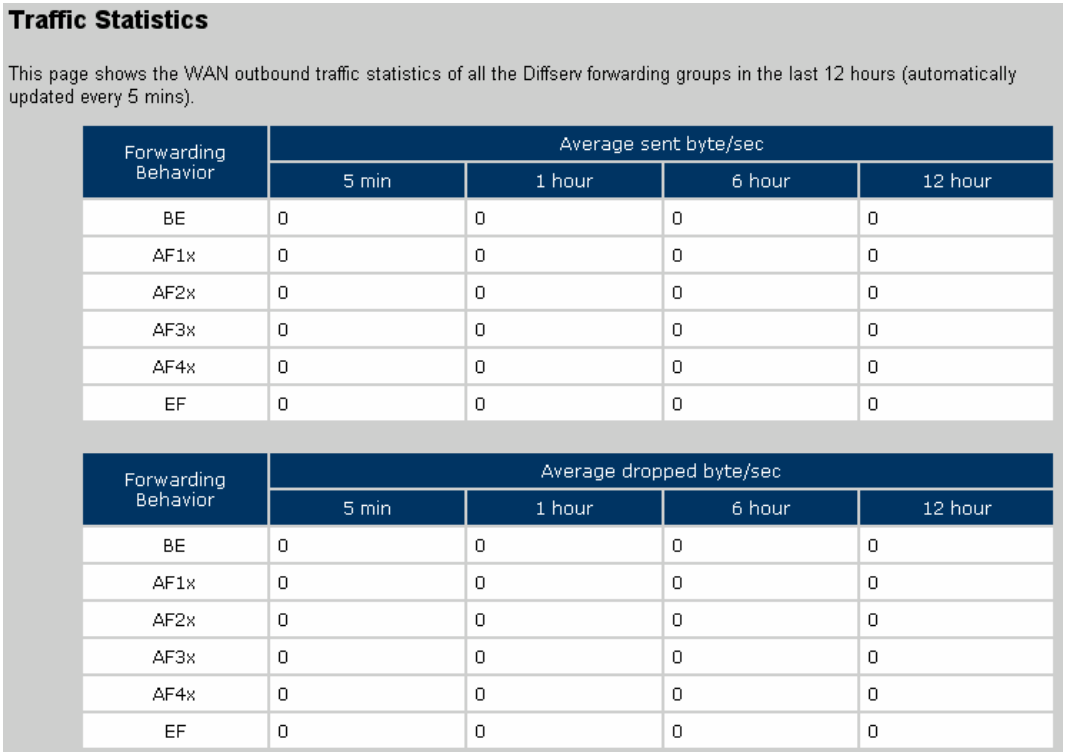
This page is for user to specify a classify rule, First, define the class by traffic type and the local and remote addresses, then set the Diffserv forwarding group this class is mapped to, finally select the outgoing VC that traffic of this class would be routed to.


Edit Traffic Class
This page is for user to specify a classify rule. First, define the class by the traffic type and the local and remote addresses. Then set the Diffserv forwarding group this class is mapped to. Finally, select the outgoing VC that traffic of this class would be routed to.
Rule Name
Traffic Type
Any
ADVANCED CONFIG
Map to Forwarding Group
BE
Remark DSCP as
BE (000000)
(the first 6 bits of IP TOS field)


Edit Traffic Class
This page is for user to specify a classify rule. First, define the class by the traffic type and the local and remote addresses. Then set the Diffserv forwarding group this class is mapped to. Finally, select the outgoing VC that traffic of this class would be routed to.
Rule Name
Local Address
Any
Remote Address
Any
Traffic Type
Any
Map to Forwarding Group
BE
Remark DSCP as
BE (000000)
(the first 6 bits of IP TOS field)

Traffic Statistics

This page shows the WAN outbound traffic statistics of all of the Diffserv forwarding groups in the last 12 hours (automatically updated every 5 mins).



Traffic Statistics

This page shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours (automatically updated every 5 mins).

Forwarding Behavior	Average sent byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

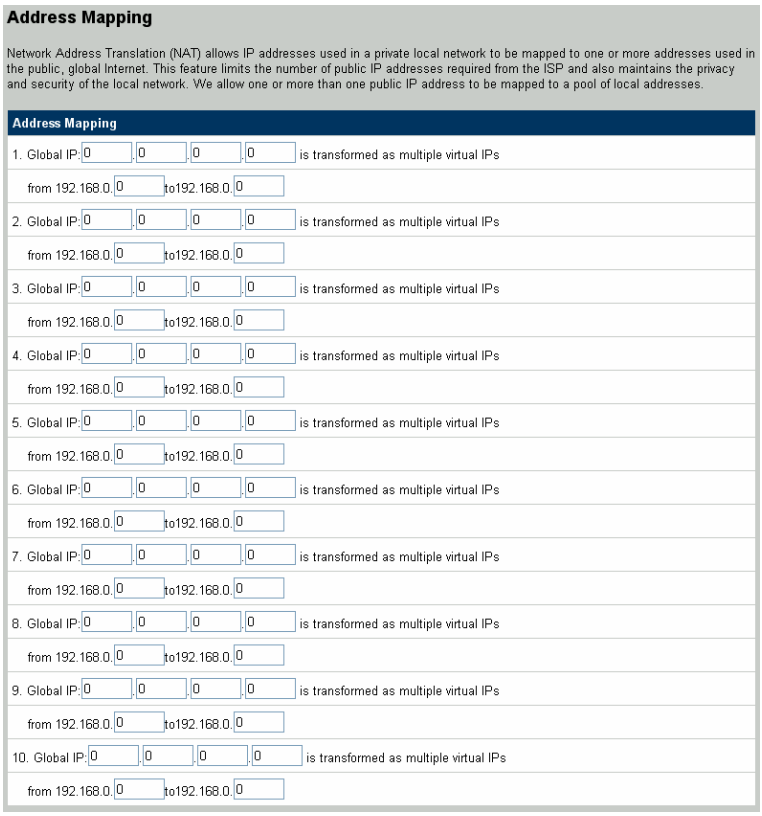
Forwarding Behavior	Average dropped byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

NAT Settings

Network Address translation (NAT) allows multipleusers at your local site to access the Internet through a signal public IP address or multiple public IP address. NAT can also prevent hacker attacks by mapping local addresses to public addresses for main services such as Web or FTP

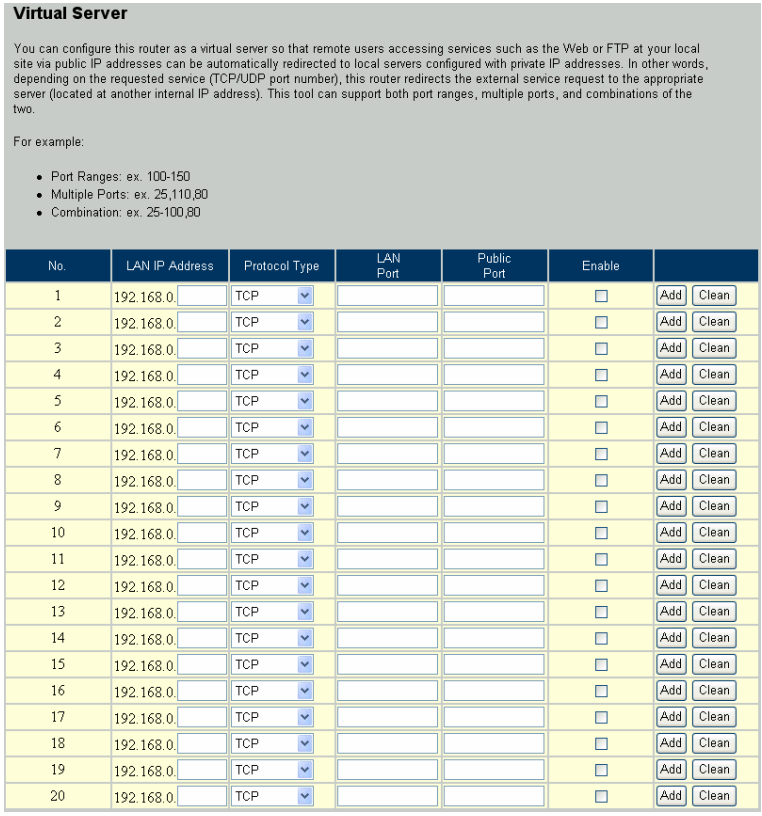
Address Mapping

VIP-462DG supports multiple global IP addresses. It allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This page allows user to enter up to 10 addresses mapping between a set of private IP addresses and one global IP address. After setting, VIP-462DG will map the set of private IP addresses to the global IP address when accessing to the Internet. This is very useful in the gaming and some particular multimedia applications.


Address Mapping
Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.
Address Mapping
1. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
2. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
3. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
4. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
5. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
6. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
7. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
8. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
9. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0
10. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.0. 0 to192.168.0. 0

Virtual Server

VIP-462DG is a NAT router. All the IP addresses coming in and going out to VIP-462DG can be converted between public and private IP addresses. You can configure VIP-462DG as a virtual server so that remote users accessing services such as the Web or FTP at your local sites via public IP address can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP), the VIP-462DG redirects the external service request to the appropriate server. After entering parameters for some application, you must press “Add” button to confirm this setting. In the other way, you also can press “Clean” button to clean all fields and ready for another parameter retrying.



Virtual Server

You can configure this router as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), this router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- Port Ranges: ex. 100-150
- Multiple Ports: ex. 25,110,80
- Combination: ex. 25-100,80

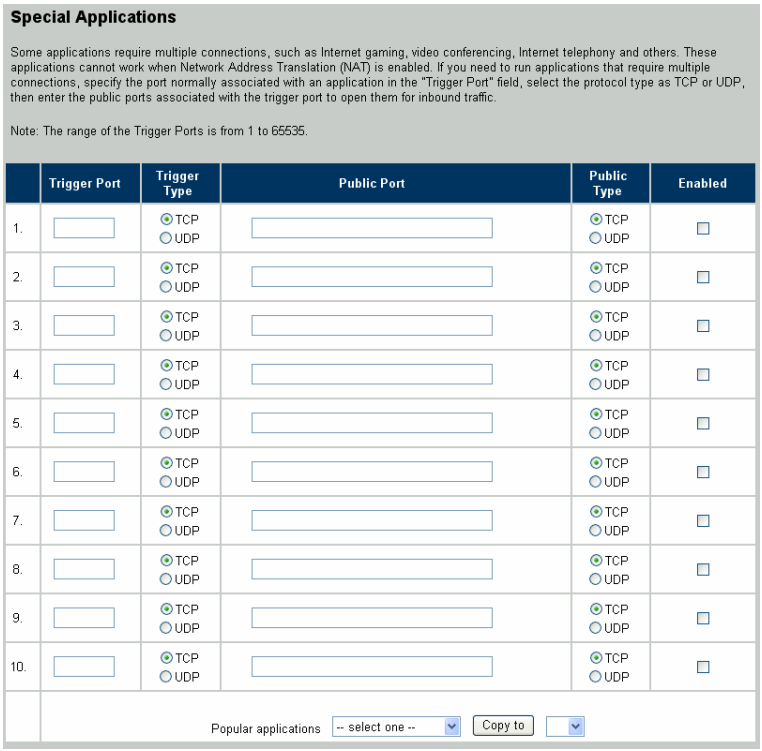
No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.0.	TCP				Add Clean
2	192.168.0.	TCP				Add Clean
3	192.168.0.	TCP				Add Clean
4	192.168.0.	TCP				Add Clean
5	192.168.0.	TCP				Add Clean
6	192.168.0.	TCP				Add Clean
7	192.168.0.	TCP				Add Clean
8	192.168.0.	TCP				Add Clean
9	192.168.0.	TCP				Add Clean
10	192.168.0.	TCP				Add Clean
11	192.168.0.	TCP				Add Clean
12	192.168.0.	TCP				Add Clean
13	192.168.0.	TCP				Add Clean
14	192.168.0.	TCP				Add Clean
15	192.168.0.	TCP				Add Clean
16	192.168.0.	TCP				Add Clean
17	192.168.0.	TCP				Add Clean
18	192.168.0.	TCP				Add Clean
19	192.168.0.	TCP				Add Clean
20	192.168.0.	TCP				Add Clean

Some of the popular applications and protocol/port numbers mapping are defined below:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Special Application

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

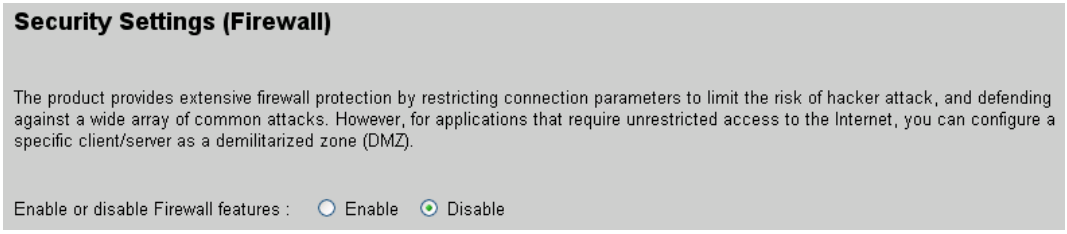

Special Applications
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.
Note: The range of the Trigger Ports is from 1 to 65535.
Trigger Port
Trigger Type
Public Port
Public Type
Enabled
TCP
UDP
Popular applications
-- select one --
Copy to

Some of the applications are listed below:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624, 28800	UDP	MSN Game Zone
2	28800	UDP	2300-2400, 47624, 28800	TCP	MSN Game Zone
3	6112	UDP	6112	UDP	Battle.net

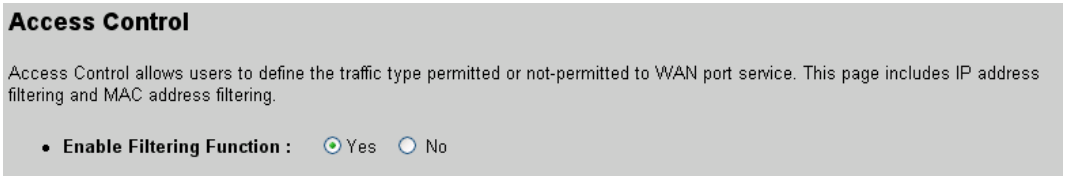
Firewall Setting

VIP-462DG provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. When firewall is enabled, extra checking will be performed for each packets passing through the device, the performance of the device will be greatly affected. To enable the firewall feature, select “Enable” from firewall page:


Security Settings (Firewall)
The product provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).
Enable or disable Firewall features : Enable Disable

Access Control

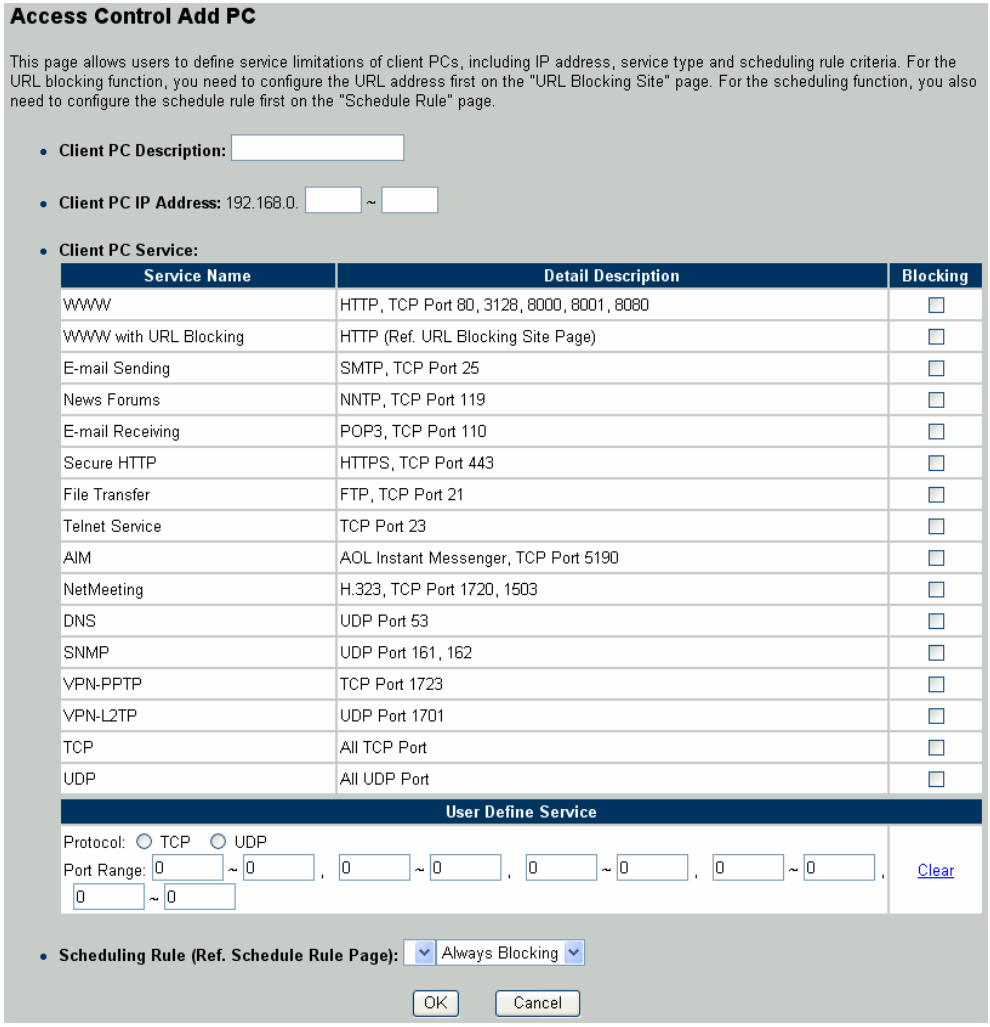
Access Control allows users to block PCs on your network from gaining access to the Internet. The user can block PCs based on IP and MAC address. When firewall is enabled, Access Control will be enabled automatically. User can disable filtering feature manually. When Access Control is enabled, all the packets will be allowed by default, user can use “Normal Filtering Table” and “MAC Filtering Table” to filter out un-allowed traffic.


Access Control
Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.
Enable Filtering Function : Yes No

Normal Filtering Table

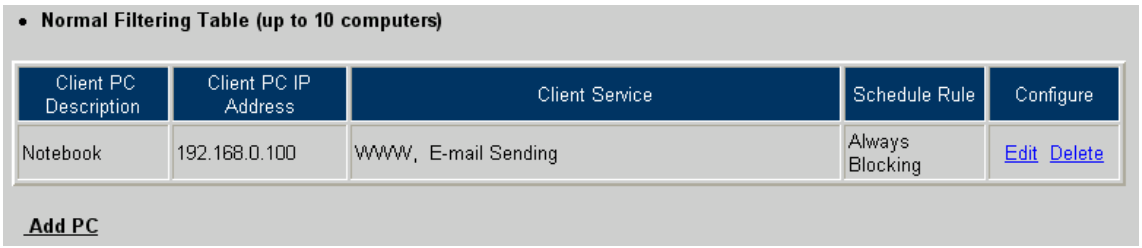
User can press “Add PC” to edit packet filtering rules.

When user select “Add PC”, the following “Access Control Add PC” page will show up:



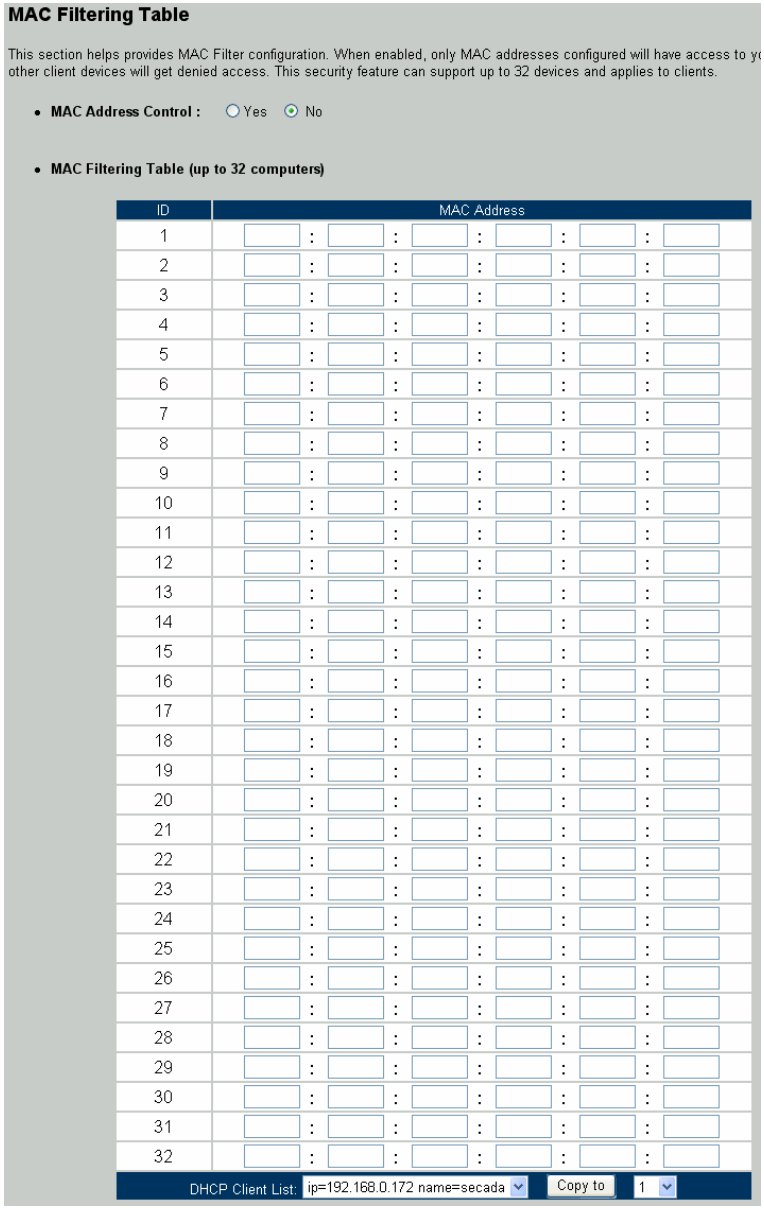
This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need config URL address first in "URL Blocking Site" page. For scheduling function, you also need config schedule rule first in "Schedule Rule" page.

As shown above, user enter Client PC Description (Notebook), and it's IP address (192.168.0.100),and select service name "WWW" and "E-mail Sending", and press "OK" button. The follow page will show up. After the setup, the PC with IP address192.168.0.100 will not be able to use WWW and sending e-mail. VIP-462DG can supports up to 32 filtering rule.



MAC Filter

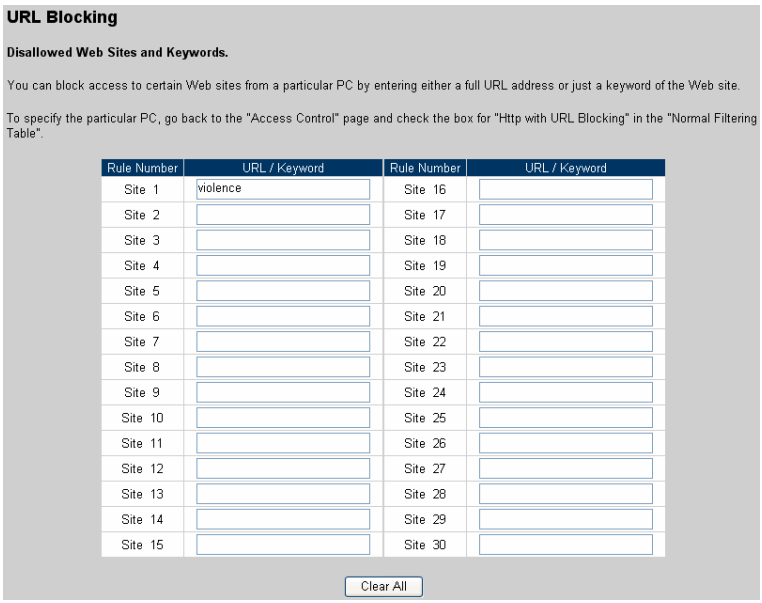
User can enter up to 32 MAC address, the PCs with these MAC addresses will not be permitted to access Internet.



URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

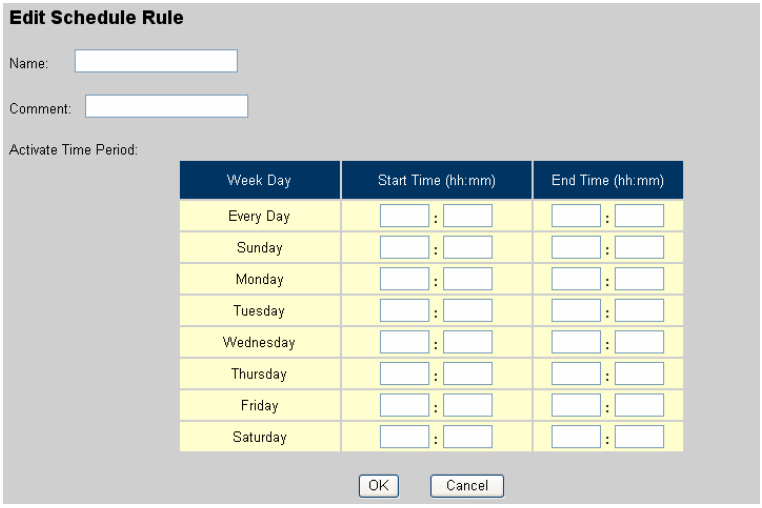


As shown above, all of the URL with ”violence” pattern cannot be accessed. The users within LAN site cannot access to any web-site with “violence” in its URL address.

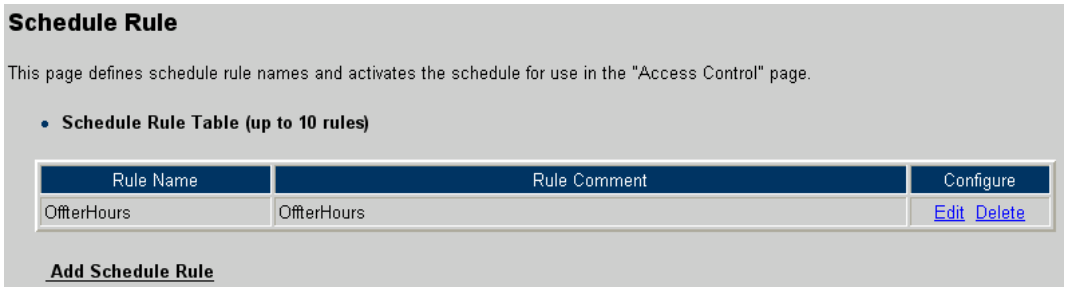
User can enter up to 32 MAC address, the PCs with these MAC addresses will not be permitted to access Internet.

Schedule Rule

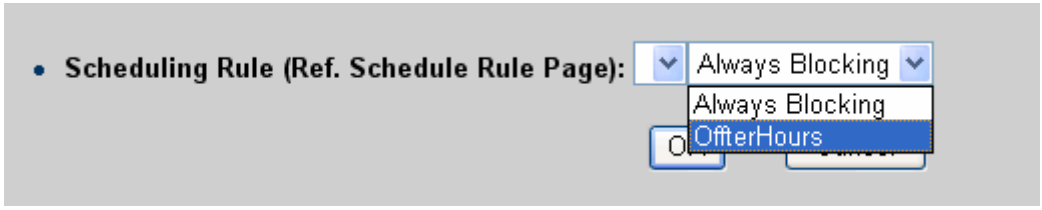
This page allows user to define schedule rule for use in Access Control page. User press “Add Schedule Rule” to add schedule name and effective time period. This defined schedule rule will be used under “Access Control Add PC”.



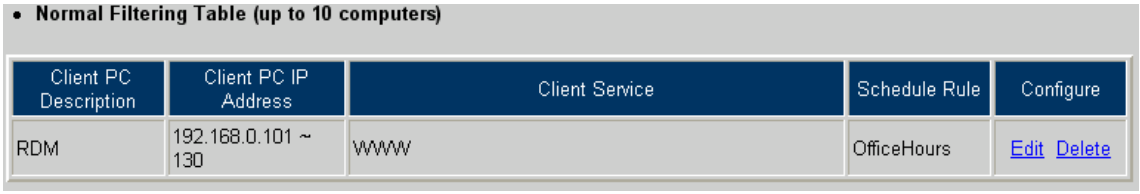
As shown above, we defined a schedule rule called “Office Hour”, the active time period is Monday to Friday, 9:00 am to 5:00 pm. After pressing “OK” button, the following page will show up:



Then when we go to “Access Control” page, select “Add PC”, in the bottom of the page “Access Control Add PC”, the scheduling rule will show “Office Hour”, as shown below:



If we setup the PC of RDM department in our company (IP address 192.168.0.101 to 192.168.0.130) can not access Web during office hour, then in “Access Control” page, we will see the following page:



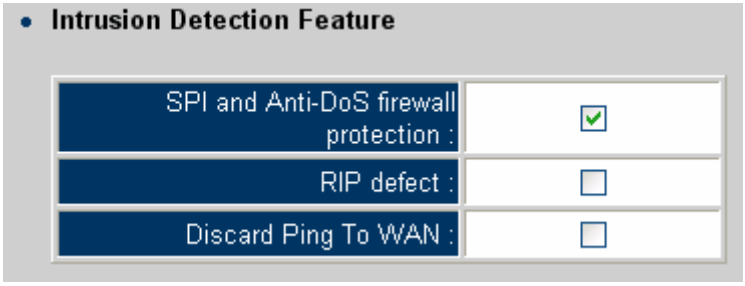
Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the product will support full operation as initiated from the local LAN.

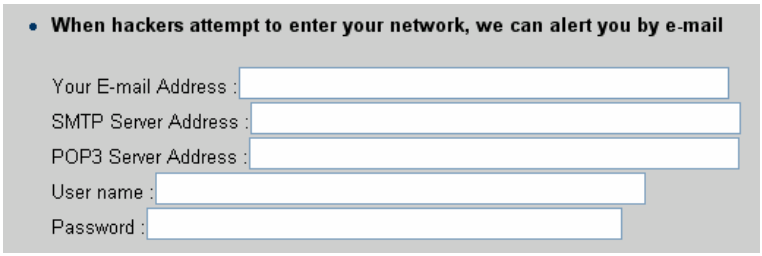
The product’s firewall can block common hacker attacks, including IP Spoofing, IP with zero length, IP With Option, Too Short ICMP, Too Short TCP, Too Short UDP, Tiny Fragment Attack, NewTear Attack, Smurf Attack, Land Attack, Ping of Death, UDP Loop Attack, Tear Drop Attack, Snork Attack, Winnuke Attack, Bonk Attack, ASCEND Probe Attack, Boink Attack, SYN Drop Attack, Empty Fragment Attack, Oshare Attack, TCP null scan, TCP Xmas scan, RIP defect, ICMP defect, TCP SYN flood, UDP flood and Fragmentation Flood.

Intrusion Detection Features:

SPI and Anti-DoS Firewall Protection	Activate SPI and Anti-DoS protection
RIP Defect	Reject the RIP packets from WAN
Discard PING from WAN	Reject all the PING request to the WAN port

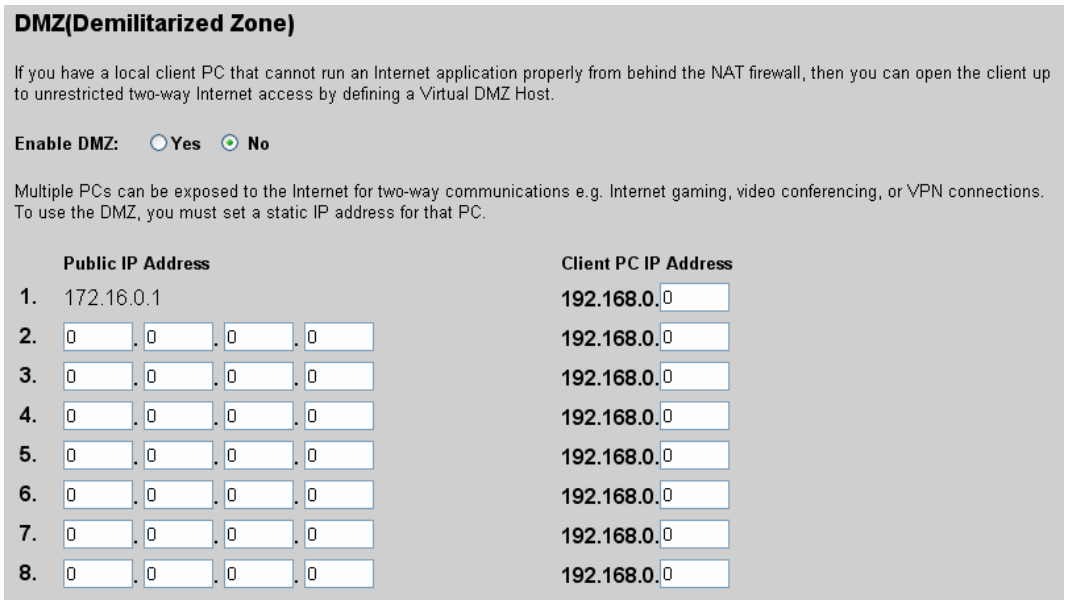


When hacker tries to attack, VIP-462DG can send e-mail alert to the specified user. Enter related e-mail information such as e-mail address and SMTP server. Some e-mail service providers require user to enter POP3 information when trying to send e-mail. In this case, enter the POP3 server, user name and password; otherwise, you don't need to enter POP3 related information.


When hackers attempt to enter your network, we can alert you by e-mail
Your E-mail Address :
SMTP Server Address :
POP3 Server Address :
User name :
Password :

DMZ

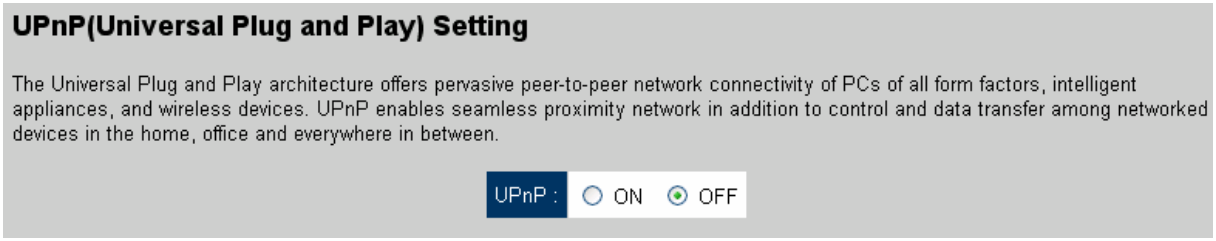
A DeMilitarized Zone (DMZ) is a network off one of the LAN ports that acts as a kind of buffer between the external (public Internet) network and your secure network on the other LAN interface. The DMZ gives access to services required from both the external network and the secure network. The services are typically HTTP/FTP (Web) servers for public access, an HTTP/FTP proxy server, an SMTP server and a News (proxy) server. Mail servers and News servers for internal use are placed on the secure network. Through the use of access control list and Firewall, you prohibit access from the Internet to your secure network while still providing access to services on the DMZ.


DMZ(Demilitarized Zone)
If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.
Enable DMZ: Yes No
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.
Public IP Address
Client PC IP Address
1. 172.16.0.1 192.168.0.0
2. 0.0.0.0 192.168.0.0
3. 0.0.0.0 192.168.0.0
4. 0.0.0.0 192.168.0.0
5. 0.0.0.0 192.168.0.0
6. 0.0.0.0 192.168.0.0
7. 0.0.0.0 192.168.0.0
8. 0.0.0.0 192.168.0.0

UPnP

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the home, office and everywhere in between.

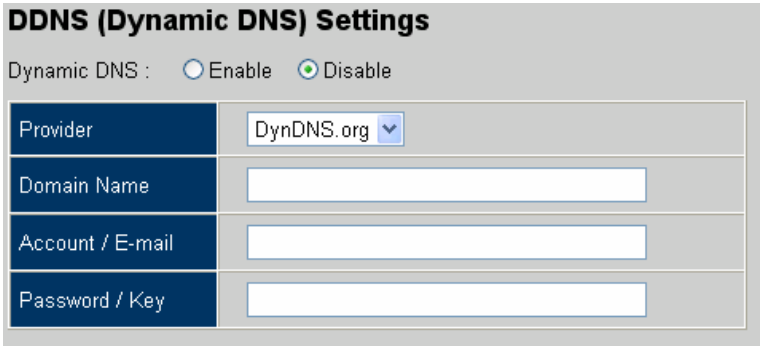
Enable the UPnP to support Windows XP network application. For example, MS Messager. If user want to use Windows XP messager application, you must enable this feature.


UPnP(Universal Plug and Play) Setting
The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the home, office and everywhere in between.
UPnP : ON OFF

DDNS

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

We can support two DDNS provider, “TZO.com” and “DynDNS.org”. You must apply DDNS service to get Key from DDNS provider and enables the DDNS service.

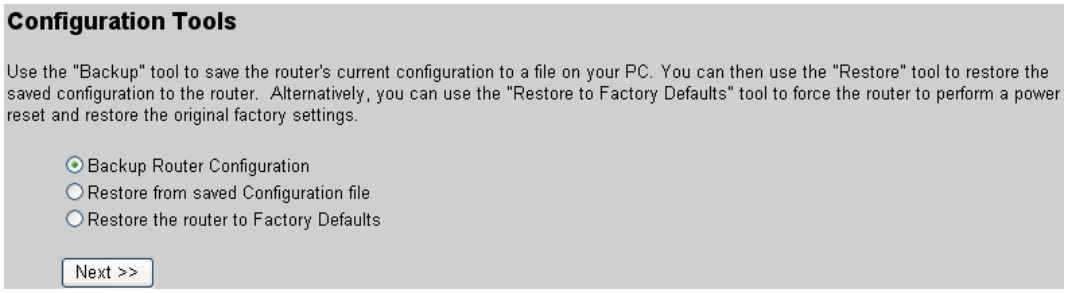


Tools

The tools feature provided by VIP-462DG includes configuration tools – save /restore configuration and restore to factory defaults, system log, firmware upgrade and reset.

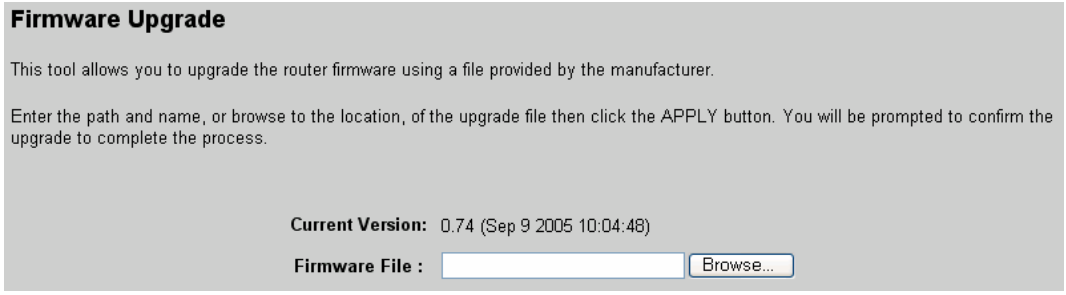
Configuration Tools

The configuration tools includes backup, restore and restore to factory defaults. The “Backup” tool save the VIP-462DG’s current configuration to a file named “backup_config.bin” on your PC. Users can then use “Restore” tool to restore the saved configuration to the VIP-462DG. The “Reset to Factory Defaults” tool will force the configuration of VIP-462DG back to the original factory setting and perform a power reset.


Configuration Tools
Use the "Backup" tool to save the router's current configuration to a file on your PC. You can then use the "Restore" tool to restore the saved configuration to the router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the router to perform a power reset and restore the original factory settings.
Backup Router Configuration
Restore from saved Configuration file
Restore the router to Factory Defaults
Next >>

Firmware Upgrade

The firmware upgrade tool allows you to upgrade the VIP-462DG system firmware. Users need to download the image file to your local PC first, and select the target file to upload.

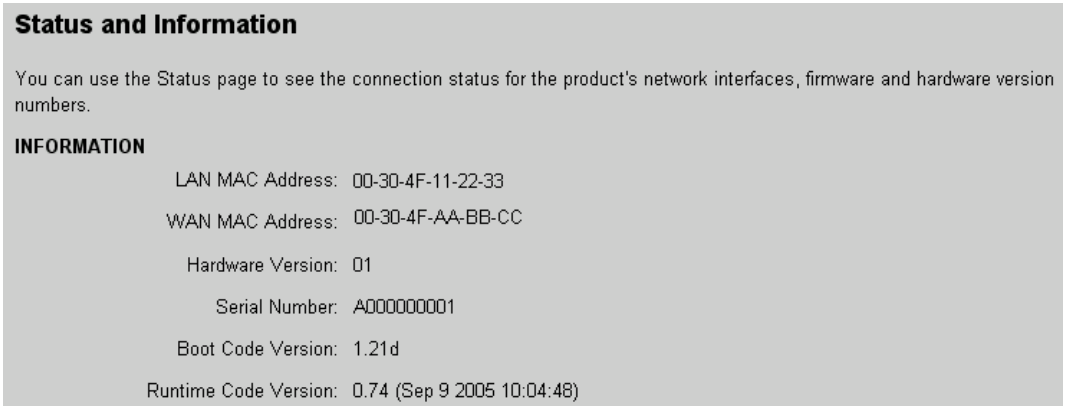

Firmware Upgrade
This tool allows you to upgrade the router firmware using a file provided by the manufacturer.
Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.
Current Version: 0.74 (Sep 9 2005 10:04:48)
Firmware File :
Browse...

Reset

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the “APPLY” button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking

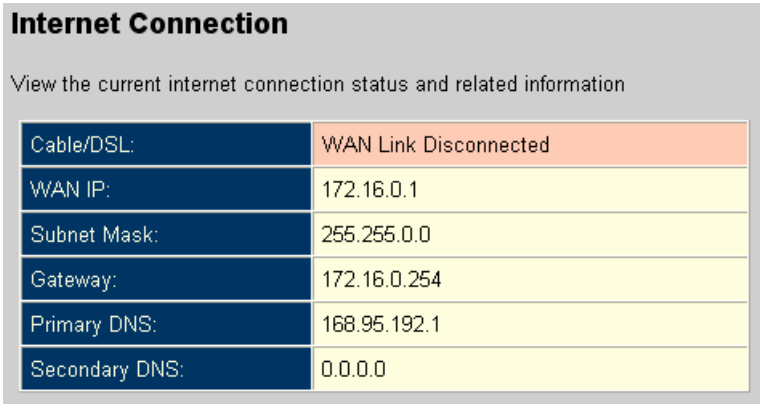
Status

The status page displays the status of the system, including the connection status of the interfaces, firmware and hardware version numbers, system log and DHCP client information.


Status and Information
You can use the Status page to see the connection status for the product's network interfaces, firmware and hardware version numbers.
INFORMATION
LAN MAC Address: 00-30-4F-11-22-33
WAN MAC Address: 00-30-4F-AA-BB-CC
Hardware Version: 01
Serial Number: A000000001
Boot Code Version: 1.21d
Runtime Code Version: 0.74 (Sep 9 2005 10:04:48)

Internet Connection

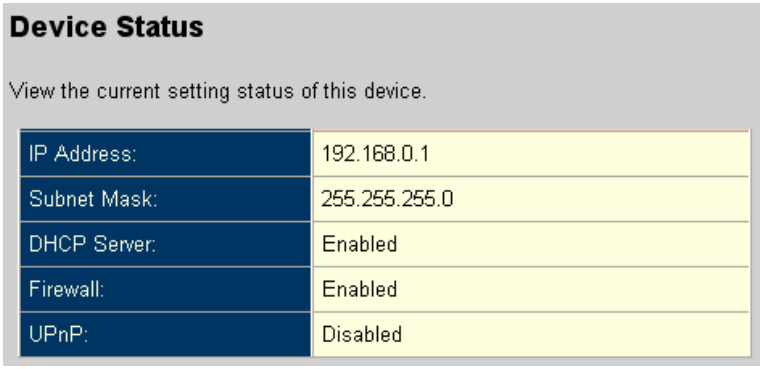
The Internet Connection page displays the status of the Internet Connection, including the connection status of the Internet interfaces, WAN port IP, Subnet Mask, Gateway IP and Primary and Secondary DNS IP.



When WAN port setting is dynamic IP, user can use “Disconnect” and “Connect” to release and update WAN port IP.

Device Status

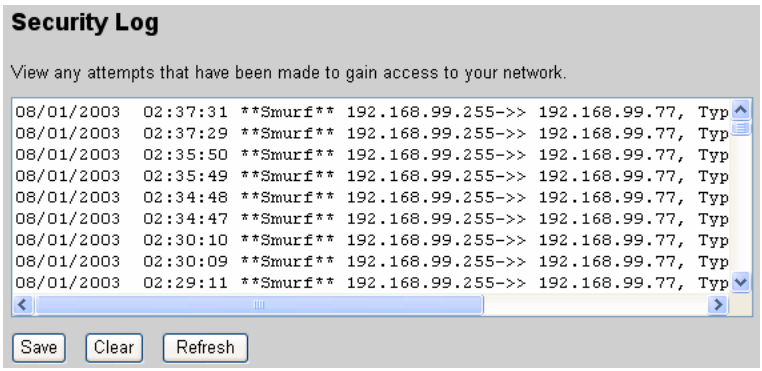
The Device Status page displays the current setting of this device, including IP address, Subnet mask, DHCP server, Firewall and UPnP.



Security Log

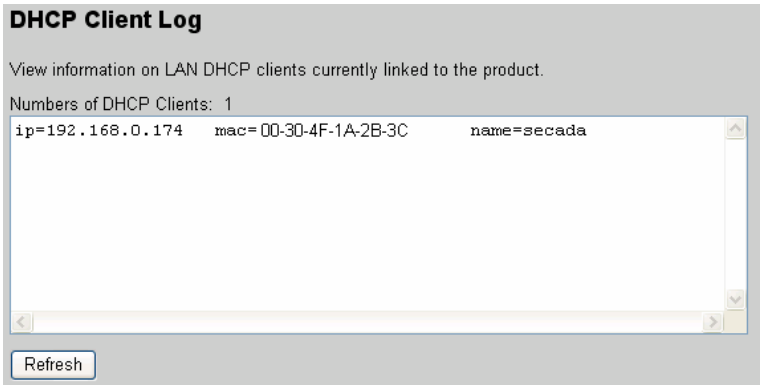
This page provides the system security log record when device boot, including user login/logout, hack attach, PPPoE connection, NTP connection, Get IP from DHCP.

These records can be saved to host PC. User also can clear all security records in Security log window and press “Refresh” button to update current security records.



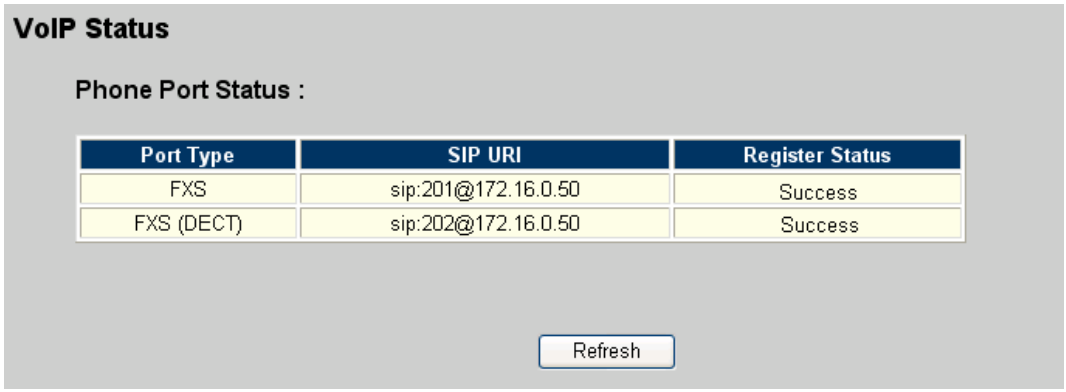
DHCP Clinet Log

The DHCP Client Log page displays the IP allocation records. User can press “Refresh” button to update current IP allocation records.


DHCP Client Log
View information on LAN DHCP clients currently linked to the product.
Numbers of DHCP Clients: 1
ip=192.168.0.174 mac=00-30-4F-1A-2B-3C name=secada
Refresh

VoIP Status

This page displays the gateway status, including Port type, port Status, time information of each call and Destination. This page also displays SIP proxy registration status. User must make sure SIP proxy registration is successful.



User can press “Refresh” button to update current VoIP status.

Appendix A

VIP-462DG Specifications

Product	802.11g SIP DECT VoIP Router
Model	VIP-462DG
Hardware	
WAN	1 x 10/100Mbps RJ-45 port
PC	4 x 10/100Mbps RJ-45 port
WLAN	IEEE 802.11b /802.11g compatible
PSTN	1 x RJ-11 connection
Phone	1 x RJ-11 connection
DECT	1 x DECT GAP compatible base
Protocols and Standard	
Standard	SIP 2.0 (RFC3261)
Voice codec	G.723.1 (6.3k/5.3k), G.729A, G.711 (A-law/U-law)
Voice Standard	Voice activity detection (VAD) Comfort noise generation (CNG) Dynamic Jitter Buffer
Supplementary services	Call transferring between DECT handsets
Protocols	RFC3261, TCP//IP, UDP/RTP/RTCP, HTTP, ICMP, ARP, DNS, DHCP, NTP/SNTP, FTP, PPP, PPPoE
Internet features	Built in NAT firewall, DoS (Denial of Service) protection QoS bandwidth management SPI (Stateful Packet Inspection) firewall Policy-based LAN/WAN access control Virtual server, DMZ, Remote administrator authentication
WLAN features	64/128 bit WEP, WPA
Network and Configuration	
Access Mode	Static IP, PPPoE, DHCP
Management	Web
Dimension (W x D x H)	237x 135 x 36 mm
Operating Environment	0~40 degree C, 10~95% humidity
Power Requirement	12V DC
EMC/EMI	CE, FCC Class B